UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/565,667	01/23/2006	Alexis S.R. Ashley	GB 030121	2467

24737 7590 03/26/2010

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
HANCE, ROBERT J	

ART UNIT	PAPER NUMBER
2421	

MAIL DATE	DELIVERY MODE
03/26/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/565,667	ASHLEY, ALEXIS S.R.	
	Examiner	Art Unit	
	ROBERT HANCE	2421	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-9,11-16 and 19-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-9,11-16 and 19-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 08 January 2010 have been fully considered but they are not persuasive.

Applicant argues on pages 17-19 of the Remarks (and argues similarly on pages 23-24 and 27-28) that the combination of Deguillaume, Penk, and Yoshida does not teach "applying ... to the hash code of combined data ... both ... a digital signature of the originator of the media data stream and ... a digital signature of a corresponding certification authority ..." In the previous rejections of claims 4, 5, and 10, these limitations were addressed as being disclosed by the Miettinen et al. and Everett et al. references. In particular, Miettinen discloses the step of applying to a hash code a digital signature of an originator of a media data stream (see [0009]), while Everett discloses the step of applying a digital signature of a certification authority (see col. 6 lines 19-33). A skilled artisan would have been motivated to combine these two teachings to increase the security of the system. Therefore the incorporation of these references into the combined system of Deguillaume, Penk, and Yoshida renders obvious previously presented claims 4, 5, and 10, and therefore renders obvious the currently amended independent claims 1, 11, 22, 31, 34 and 35.

Applicant argues on page 19 (and repeats the argument on pages 24 and 28) that the combination of references is improper because the references themselves “do not provide any incentive or motivation supporting the desirability of the combination."

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the rationale for combining the references does not come from an express statement of desirability in their combination; rather, it comes from knowledge generally available to one of ordinary skill in the art. These rationales were stated in the rejections found in the previous Office Action, and are repeated below.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-3, 6-9, 31-33 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deguillaume et al., US Pub No 2003/0070075 in view of Penk et al., US Pub No 2003/0074670 in view of Yoshida, Japanese Pub No. JP 200165248, in view of Miettinen et al., US Pub No 2002/0138729 and further in view of Everett, US Patent No 6,328,217.

As to claim 1 Deguillaume discloses a method for providing content identification within media data for distribution from a media content data source device comprising:

inserting content identification data into frames of the media data stream to be distributed, in conjunction with each data frame for which corresponding content identification data relates, wherein the content identification data includes a tamper resistant identifier that is based upon a rapidly changing property extracted from a given data frame of the media data that is difficult to alter and is inserted into the media data stream in conjunction with the corresponding given data frame by reference to the rapidly changing property from which property data was extracted (Paragraphs 33-35 and 40-42; claims 12 and 13; Figs. 1 and 2 – watermarks are embedded in frames of video. The watermarks are dependent on the information in the frame of video, and therefore are a form of content identification – see for example the extraction and

verification process described in Paragraphs 45-48. Due to the nature of video, these tamper resistant identifiers are based on rapidly changing properties of the media data. The watermarks are embedded in conjunction with the video frame from which the identification data is extracted. This watermark is (i) difficult to alter and (ii) inserted in conjunction with the corresponding given data frame by referring to the rapidly changing (image) property. See Paragraphs 40-42)

extracting data relating to a predetermined property of the media data stream (Paragraphs 40-42);

combining the extracted data with content identification data by forming a hash code from the extracted data and the content identification data (Paragraphs 40-42 – unique image identification name or number, etc. is included in the input to the hash function); and

inserting the combined data and a digital signature as secured content identification data into the data stream (Paragraphs 20 and 34).

Deguillaume fails to disclose that the content identification is inserted within the media data stream; and receiving the data stream of media content at the media content data source device.

However, in an analogous art, Penk discloses a broadcaster which receives a data stream of media content (Paragraph 41; Fig. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Deguillaume with the teachings of Penk. In the combined system of Deguillaume and Penk, the data stored at the broadcaster (Penk

Fig. 2: 102) is a stored stream, therefore the content identification is inserted within a media data stream. The rationale for this modification would have been to enable the invention of Deguillaume to receive media content from a remote content provider.

The combined system of Deguillaume and Penk fail to disclose that the content identification is inserted at regular intervals within the media data stream; that the rapidly changing property of the media data stream includes a property which changes with each frame of the media data stream; and the content identification data further comprising a continuity count within the identifier, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count.

However, in an analogous art, Yoshida discloses content identification inserted at regular intervals within the media data stream (Abs – watermarks are inserted at each frame);

that the rapidly changing property of the media data stream used to calculated a watermark includes a property which changes with each frame of the media data stream (Abs – watermarks are based on frame number, which changes with each frame); and

content identification data inserted into frames of a media data stream that comprises a continuity count, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count (Abs – the watermark comprises frame number, or a

continuity count, which increments with each frame. Watermarks are inserted at each frame, so the count is incremented each time the identifier is inserted into the stream).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combined system of Deguillaume and Penk with the teachings of Yoshida. The rationale for this modification would have been to provider further protection of copyright of contents against interception by providing an even more secure watermarking scheme.

The combined system of Deguillaume, Penk and Yoshida disclose fail to disclose applying a digital signature to the combined data.

However, Miettinen et al. disclose applying a digital signature to a hash code that includes applying a digital signature of the originator of a media data stream (Paragraph 9).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the digital signature disclosed by Miettinen et al. in the combined system of Deguillaume, Penk and Yoshida. The rationale for this combination would have been to ascertain whether the data being sent had been modified (see Miettinen et al. Paragraph 9).

The combined system of Deguillaume, Penk, Yoshida and Miettinen fail to disclose that step of applying a digital signature to the hash code further includes applying digital signatures of the originator of the media data stream and a certification authority.

However, in an analogous art, Everett et al. disclose applying a digital signature of a certification authority (col. 6 lines 19-33). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the signatures method disclosed by Everett et al. in the system of Deguillaume, Penk, Yoshida and Miettinen. The rationale for this combination would have been to assure the identity of the originator of the media data stream.

As to claim 2 the combined system of Deguillaume, Penk, Yoshida, Miettinen and Everett disclose the method of claim 1 wherein the content identification data is inserted every frame (Yoshida Abs).

As to claim 3 the combined system of Deguillaume, Penk, Yoshida, Miettinen and Everett disclose the method of claim 1 wherein the content identification data is digitally combined with a predetermined property of the data stream (Deguillaume Paragraphs 40-42).

As to claim 6 the combined system of Deguillaume, Penk, Yoshida, Miettinen and Everett disclose the method of claim 1 in which the media data stream may comprise any one or more of pictures and audio or video data streams (Penk Paragraph 40).

As to claim 7 the combined system of Deguillaume, Penk, Yoshida, Miettinen and Everett disclose a method in which the predetermined property is any property of the media data stream that changes from data frame to data frame (Deguillaume Paragraph 40 – the hash function takes as its input the data of local blocks of video (see claim 12-13), which by nature changes from frame to frame).

As to claim 8 the combined system of Deguillaume, Penk, Yoshida, Miettinen and Everett disclose a method in which the predetermined property comprises any one or more of: frame size, frame hash, transport stream identifier, clock signal, and continuity count (Deguillaume Paragraphs 40-42).

As to claim 9 the combined system of Deguillaume, Penk, Yoshida, Miettinen and Everett disclose a method in which the predetermined property is a combination of frame size and frame hash (Deguillaume Paragraphs 40-42).

As to claims 31 and 36, see similar rejection of claim 1. The method of claim 1 corresponds to the apparatus of claim 31 and the computer program products of claim 36. Therefore, claims 31 and 36 have been analyzed and rejected.

As to claim 32 see similar rejection of claim 1. The method of claim 1 corresponds to the apparatus of claim 32. Therefore claim 32 has been analyzed and rejected.

As to claim 33 Deguillaume, Penk, Yoshida, Miettinen and Everett disclose the apparatus of claim 32 in which the means for combining includes a hash function generator for forming a hash code from the combined data, the encryption module applying the digital signature to the hash code (Deguillaume Paragraphs 40-42; Miettinen [0009]).

3. Claims 11-16 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chang et al., US Patent No 6,963,972 in view of Deguillaume, in view of Yoshida,

in view of Miettinen, in view of Everett, and further in view of Reeds et al., US Patent No 5,153,919.

As to claim 11 Chang et al. disclose a method of transcoding a media data stream for distribution from a transcoder device, the method comprising:

receiving a data stream of media content from a media content data source (col. 7 lines 39-58; Fig. 8); transcoding the media content of the data stream into a new format (col. 7 lines 39-58).

Chang et al. fail to disclose that the media stream includes embedded, secured content identification data in frames of the media data stream, in which the secured content identification data incorporates data relating to a predetermined property of the media data stream and that corresponds to a tamper resistant identifier that is based upon a rapidly changing property of the media data stream; extracting data relating to a predetermined property of the media data stream in its new format; extracting content identification data from the secured content identification data; and combining the extracted data with the extracted content identification data.

However, in an analogous art, Deguillaume et al. disclose

a media stream that includes embedded, secured content identification data in frames, in conjunction with each data frame for which a corresponding content identification data relates, in which the secured content identification data incorporates data relating to a predetermined property of the media data stream and that corresponds to a tamper resistant identifier that is based upon a rapidly changing property extracted from a given data frame of the media data that is difficult to alter and

is inserted into the media data in conjunction with the corresponding given data frame by reference to the rapidly changing property from which property data was extracted (Paragraphs 33-35 and 40-42; claims 12 and 13; Figs. 1 and 2 – watermarks are embedded in frames of video. The watermarks are dependent on the information in the frame of video, and therefore are a form of content identification – see for example the extraction and verification process described in Paragraphs 45-48. Due to the nature of video, these tamper resistant identifiers are based on rapidly changing properties of the media data. The watermarks are embedded in conjunction with the video frame from which the identification data is extracted. This watermark is (i) difficult to alter and (ii) inserted in conjunction with the corresponding given data frame by referring to the rapidly changing (image) property. See Paragraphs 40-42);

extracting data relating to a predetermined property of the media data stream (Paragraphs 40-42);

extracting content identification data from the secured content identification data (Paragraphs 45-46 – the watermark, which contains content identification data, is decrypted and extracted); and

combining the extracted data with content identification data by forming a hash code from the extracted data and the content identification data (Paragraphs 40-42 – unique image identification name or number, etc. is included in the input to the hash function); and

inserting the combined data and a digital signature as secured content identification data into the data stream (Paragraphs 20 and 34).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the encryption method disclosed by Deguillaume et al. in the transcoder disclosed by Chant et al. The rationale for this combination would have been to create a more secure hash code that contains local contextual dependencies, thus making it more difficult to forge (Deguillaume Paragraph 40-42). All of the functions disclosed by Deguillaume et al. could have been easily applied to the data stream after it was transcoded.

The combined system of Chang and Deguillaume fails to disclose that identification data is inserted at regular intervals within the media data stream; the rapidly changing property of the media data stream includes a property which changes with each frame of the media data stream; the content identification data further including a continuity count within the identifier, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count.

However, in an analogous art, Yoshida discloses content identification inserted at regular intervals within the media data stream (Abs – watermarks are inserted at each frame);

that the rapidly changing property of the media data stream used to calculated a watermark includes a property which changes with each frame of the media data stream (Abs – watermarks are based on frame number, which changes with each frame); and

content identification data inserted into frames of a media data stream that comprises a continuity count, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count (Abs – the watermark comprises frame number, or a continuity count, which increments with each frame. Watermarks are inserted at each frame, so the count is incremented each time the identifier is inserted into the stream).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combined system of Chang and Deguillaume with the teachings of Yoshida. The rationale for this modification would have been to provider further protection of copyright of contents against interception by providing an even more secure watermarking scheme.

The combined system of Chang, Deguillaume and Yoshida fail to disclose applying a digital signature to the combined data.

However, in an analogous art, Miettinen et al. disclose applying a digital signature to a hash code (Paragraph 9). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the digital signature disclosed by Miettinen et al. in the combined system of Chang, Deguillaume and Yoshida. The rationale for this combination would have been to ascertain whether the data being sent had been modified (see Miettinen et al. Paragraph 9). Therefore it would have been obvious to insert the combined data (as disclosed by Deguillaume et al.) and digital

signature (as disclosed by Miettinen et al.) as re-secured content identification data into the data stream.

The combined system of Chang, Deguillaume, Yoshida and Miettinen fail to disclose that step of applying a digital signature to the hash code further includes applying digital signatures of the originator of the media data stream and a certification authority.

However, in an analogous art, Everett et al. disclose applying a digital signature of a certification authority (col. 6 lines 19-33). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the signatures method disclosed by Everett et al. in the system of Deguillaume, Penk, Yoshida and Miettinen. The rationale for this combination would have been to assure the identity of the originator of the media data stream.

The combined system of Chang, Deguillaume, Yoshida, Miettinen and Everett fail to disclose the method of claim 17 in which the step of applying a digital signature to the combined data further includes the step of making available a corresponding public key of the transcoding device that is digitally signed by the originator of the content identification data.

However, in an analogous art, Reeds et al. disclose making available the public key of a device that is digitally signed by the originator of the content identification data to prove to third parties that the device is authorized by the content provider (col. 2 lines 17-27).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the public key as disclosed by Reeds et al. in the transcoder of Chang et al. as modified. The rationale for this combination would have been to assure third parties that the transcoder is authorized by the content provider.

As to claim 12 the combined system of Chang, Deguillaume, Yoshida, Miettinen, Everett and Reeds disclose a method in which the new format of the data stream has a lower resolution or transmission/storage bandwidth than the original format of the data stream (Chang col. 1: 43-62).

As to claim 13 the combined system of Chang, Deguillaume, Yoshida, Miettinen, Everett and Reeds disclose a method in which the media content may comprise audio and video data streams (Chang col. 1:15-30).

As to claim 14 the combined system of Chang, Deguillaume, Yoshida, Miettinen, Everett and Reeds disclose the method of claim 11 in which the predetermined property is any property of the media data stream that changes from data frame to data frame (Deguillaume Paragraph 40-42).

As to claim 15 the combined system of Chang, Deguillaume, Yoshida, Miettinen, Everett and Reeds disclose the method of claim 14 in which the predetermined property comprises frame size and frame hash (Deguillaume Paragraph 40-42).

As to claim 16 the combined system of Chang, Deguillaume, Yoshida, Miettinen, Everett and Reeds disclose the method of claim 15 in which the predetermined property is a combination of frame size and frame hash (Deguillaume Paragraphs 40-42).

As to claim 34 see similar rejection of claim 11. The method of claim 11 corresponds to the apparatus of claim 34. Therefore, claim 34 has been analyzed and rejected.

4. Claims 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chang, Deguillaume, Yoshida, Miettinen, Everett and Reeds as applied to claim 11 above, and further in view of McCormack et al., US Pub No 2004/0143836.

As to claim 19 the combined system of Chang, Deguillaume, Yoshida, Miettinen, Everett and Reeds fail to disclose the method of claim 11 in which the step of combining the extracted data with the extracted content identification data further includes the step of modifying the extracted content identification data.

However, in an analogous art, McCormack et al. disclose updating meta data (i.e. content identification data) after transcoding (Paragraph 76).

It would have been obvious to one of ordinary skill in the art at the time of the invention to update the content identification data as disclosed by McCormack et al. in the transcoder of the combined system of Chang, Deguillaume, Yoshida, Miettinen, Everett and Reeds. The rationale for this combination would have been to pass on updated meta data that reflects the changes made by the transcoder. All the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

As to claim 20 the combined system of Chang, Deguillaume, Yoshida, Miettinen, Everett, Reeds and McCormack disclose the method of claim 19 in which the step of modifying the extracted content identification data comprises including an indication of the new format of the transcoded data stream (McCormack Paragraph 76).

As to claim 21 the combined system of Chang, Deguillaume, Yoshida, Miettinen, Everett, Reeds and McCormack disclose the method of claim 19 in which the step of modifying the extracted content identification data comprises including an identity of a device performing the transcoding (McCormack Paragraph 76 - transcoding device is identified in the updated meta data).

5. Claims 22-24, 27-30 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deguillaume in view of Yoshida in view of Miettinen and further in view of Everett.

As to claim 22 Deguillaume et al. disclose a method of verifying the integrity of secured content identification data embedded in a media data stream with a receiver device, comprising the steps of:

receiving a data stream of media content by the receiver device (content can be video - see claims 12-13) the data stream of media content including embedded, secured content identification data in frames of the media data stream, in conjunction with each data frame for which a corresponding content identification data relates, in which the secured content identification data incorporates data relating to a predetermined property of the media data stream and that corresponds to a tamper

resistant identifier that is based upon a rapidly changing property extracted from a given data frame of the media data stream that is difficult to alter and is inserted into the media data stream in conjunction with the corresponding given data frame by reference to the rapidly changing property from which property data was extracted (Paragraphs 33-35 and 40-42; claims 12 and 13; Figs. 1 and 2 – watermarks are embedded in frames of video. The watermarks are dependent on the information in the frame of video, and therefore are a form of content identification – see for example the extraction and verification process described in Paragraphs 45-48. Due to the nature of video, these tamper resistant identifiers are based on rapidly changing properties of the media data. The watermarks are embedded in conjunction with the video frame from which the identification data is extracted. This watermark is (i) difficult to alter and (ii) inserted in conjunction with the corresponding given data frame by referring to the rapidly changing (image) property. See Paragraphs 40-42);

extracting first data relating to a predetermined property of the media data stream (Paragraphs 45-48 - a signature is recalculated from the received data);

extracting content identification data from the secured content identification data (Paragraphs 45-48 – content identification data is contained within the extracted watermark. See paragraphs 40-42);

extracting second data relating to the predetermined property from the secured content identification data (Paragraphs 45-48 - the encrypted, embedded signature is extracted); and

comparing the first data and the second data to verify the authenticity of the extracted content identification data (Paragraph 46 – the computed signature is compared with the extracted signature, and A_T is the result of the comparison);

extracting data relating to a predetermined property of the media data stream (Paragraphs 40-42);

combining the extracted data with content identification data by forming a hash code from the extracted data and the content identification data (Paragraphs 40-42 – unique image identification name or number, etc. is included in the input to the hash function); and

inserting the combined data and a digital signature as secured content identification data into the data stream (Paragraphs 20 and 34).

Deguillaume fails to disclose the content identification is inserted at regular intervals within the media data stream; that the rapidly changing property of the media data stream includes a property which changes with each frame of the media data stream; and the content identification data further comprising a continuity count within the identifier, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count.

However, in an analogous art, Yoshida discloses content identification inserted at regular intervals within the media data stream (Abs – watermarks are inserted at each frame);

that the rapidly changing property of the media data stream used to calculated a watermark includes a property which changes with each frame of the media data stream (Abs – watermarks are based on frame number, which changes with each frame); and

content identification data inserted into frames of a media data stream that comprises a continuity count, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count (Abs – the watermark comprises frame number, or a continuity count, which increments with each frame. Watermarks are inserted at each frame, so the count is incremented each time the identifier is inserted into the stream).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Deguillaume with the teachings of Yoshida. The rationale for this modification would have been to provider further protection of copyright of contents against interception by providing an even more secure watermarking scheme.

The combined system of Deguillaume and Yoshida disclose fail to disclose applying a digital signature to the combined data.

However, Miettinen et al. disclose applying a digital signature to a hash code that includes applying a digital signature of the originator of a media data stream (Paragraph 9).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the digital signature disclosed by Miettinen et al. in the combined

system of Deguillaume and Yoshida. The rationale for this combination would have been to ascertain whether the data being sent had been modified (see Miettinen et al. Paragraph 9).

The combined system of Deguillaume, Yoshida and Miettinen fail to disclose that step of applying a digital signature to the hash code further includes applying digital signatures of the originator of the media data stream and a certification authority.

However, in an analogous art, Everett et al. disclose applying a digital signature of a certification authority (col. 6 lines 19-33). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the signatures method disclosed by Everett et al. in the system of Deguillaume, Yoshida and Miettinen. The rationale for this combination would have been to assure the identity of the originator of the media data stream.

As to claim 23 the combined system of Deguillaume, Yoshida, Miettinen and Everett disclose the method of claim 22 in which the step of extracting content identification data from the secured content identification data comprises the steps of: obtaining a public key of a content provider that secured the content identification data; and verifying an encrypted signature of the content provider using the public key (Miettinen Paragraph 9).

As to claim 24 the combined system of Deguillaume, Yoshida, Miettinen and Everett disclose the method of claim 23 in which the step of extracting content identification data from the secured content identification data comprises the steps of: obtaining a public key of a certification authority; verifying the authenticity of the public

key of the content provider using the public key of the certification authority (Everett col. 6 lines 19-33).

As to claim 27 the combined system of Deguillaume, Yoshida, Miettinen and Everett discloses the method of claim 22 in which the media content data stream comprises pictures, audio, video data streams (Deguillaume Paragraph 33, Claims 12-13).

As to claim 28 the combined system of Deguillaume, Yoshida, Miettinen and Everett disclose the method of claim 22 in which the predetermined property is any property of the media data stream that changes from data frame to data frame (Deguillaume Paragraphs 40-42).

As to claim 29 the combined system of Deguillaume, Yoshida, Miettinen and Everett disclose the method of claim 28 in which the predetermined property comprises frame size and frame hash (Deguillaume Paragraphs 40-42).

As to claim 30 the combined system of Deguillaume, Yoshida, Miettinen and Everett disclose the method of claim 29 in which the predetermined property is a combination of frame size and frame hash (Deguillaume Paragraphs 40-42).

As to claim 35 see similar rejection of claim 22. The method of claim 22 corresponds to the apparatus of claim 35. Therefore, claim 35 has been analyzed and rejected.

6. Claims 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deguillaume, Yoshida, Miettinen and Everett as applied to claim 22 above, and further

in view of Chang et al., US Patent No 6,963,972 and further in view of Reeds et al., US Patent No 5,153,919.

As to claim 25 the combined system of Deguillaume, Yoshida, Miettinen and Everett fail to disclose the method of claim 22 in which the media data stream is received via a transcoding device, and in which the step of extracting content identification data from the secured content identification data comprises the steps of verifying that the transcoder device was authorised to modify the data stream by an originator of the content identification data.

However, in an analogous art, Chang et al. disclose that the media data stream is received via a transcoding proxy device (col. 7 lines 39-58, Fig. 8)

It would have been obvious to one of ordinary skill in the art at the time of the invention to use a transcoding device as disclosed by Chang et al. in the encryption scheme disclosed by Deguillaume, Yoshida, Miettinen and Everett. The rationale for this combination would have been to change the format of data when necessary.

The combined system of Deguillaume, Yoshida, Miettinen, Everett and Chang fails to disclose verifying that the transcoder device was authorised to modify the data stream by an originator of the content identification data.

However, in an analogous art, Reeds et al. disclose making available the public key of a device that is digitally signed by the originator of the content identification data to prove to third parties that the device is authorized by the content provider (col. 2 lines 17-27).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the digital signature disclosed by Reeds et al. in the transcoder of the combined system of Deguillaume, Yoshida, Miettinen, Everett and Chang. The rationale for this combination would have been to assure that the transcoder is trustworthy.

As to claim 26 the combined system of Deguillaume, Yoshida, Miettinen, Everett, Chang and Reeds disclose the method of claim 25 in which the step of extracting content identification data from the secured content identification data comprises

obtaining a public key of the transcoding device that secured the content identification data, the public key being digitally signed by the originator of the content identification data (Reeds col. 2 lines 17-28).

obtaining a public key of the originator; verifying an encrypted signature of the originator using the public key of the originator, and thereby verifying the public key of the transcoder device; verifying the content identification information using the verified public key of the transcoder device (Miettinen Paragraph 9).

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ROBERT HANCE whose telephone number is (571)270-5319. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John W. Miller can be reached on (571) 272-7353. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/John W. Miller/ ROBERT HANCE

Supervisory Patent Examiner, Art Unit 2421

Examiner
Art Unit 2421

/ROBERT HANCE/
Examiner, Art Unit 2421